A Cloud Reference Architecture Based on NIST Cybersecurity Framework

DIR Technology Forum 2017

Bo Lane, Head of Security Architecture

Introduction

- Widespread adoption of cloud services
- Shared control and security responsibility
- Increase in cloud-based cyber-attacks
- Increasingly crowded cloud security market

KUDELSKI SECURITY

Cloud Threats, Impacts & Challenges

The **critical role** of public cloud platforms and the **interconnected dependencies** that they create.

Cloud Threats, Impacts & Challenges

Through 2020,
95 percent of cloud security failures
will be the customer's fault. (Gartner)

KUDELSKI SECURITY

Cloud Threats, Impacts & Challenges

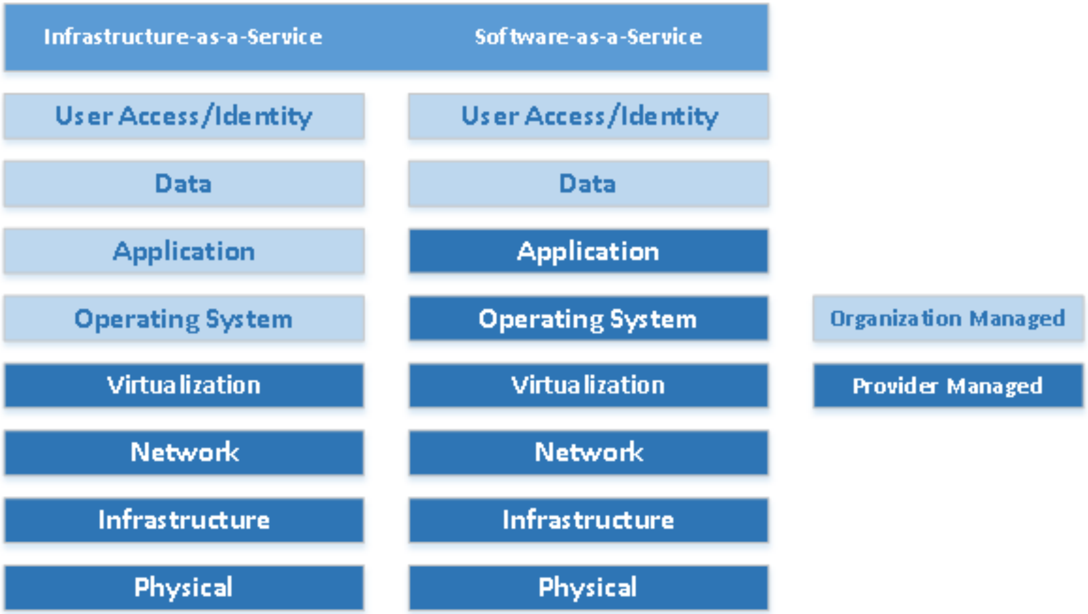
According to a recent Symantec survey, most CIOs think their organizations only use around 30 or 40 cloud apps. However, the average enterprise organization was using almost 930 cloud apps, up from 841 earlier in 2016.

Shared Security Responsibility

Security *of* the cloud

vs.

Security *in* the cloud



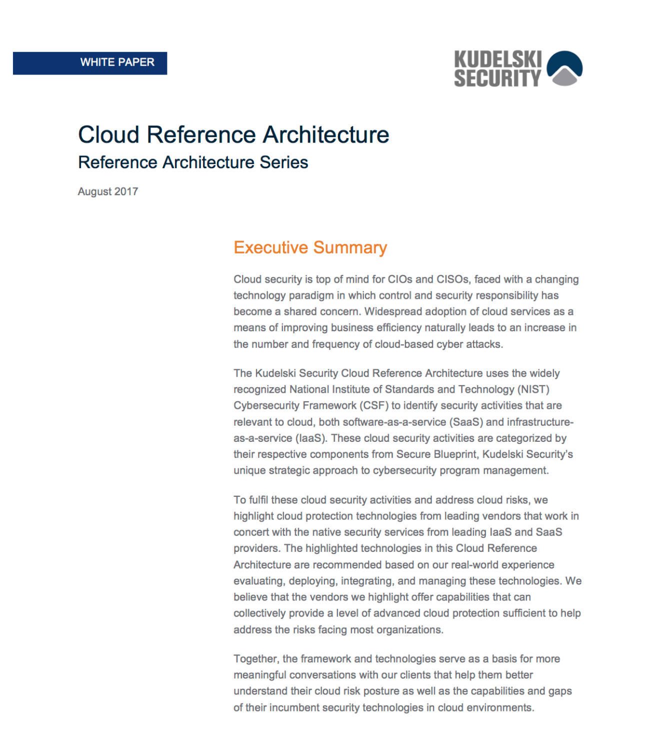
Infrastructure-as-a-Service	Software-as-a-Service
User Access/Identity	User Access/Identity
Data	Data
Application	Application
Operating System	Operating System
Virtualization	Virtualization
Network	Network
Infrastructure	Infrastructure
Physical	Physical

Organization Managed

Provider Managed

Cloud Reference Architecture

- Advice and Technology Recommendations
- NIST Cybersecurity Framework
- Kudelski Security's Secure Blueprint
- Clean-Sheet Technology Approach
- Compliment Native IaaS/SaaS Security Tools
- Cloud-Focused Policy is Vital



WHITE PAPER

KUDELSKI SECURITY

Cloud Reference Architecture

Reference Architecture Series

August 2017

Executive Summary

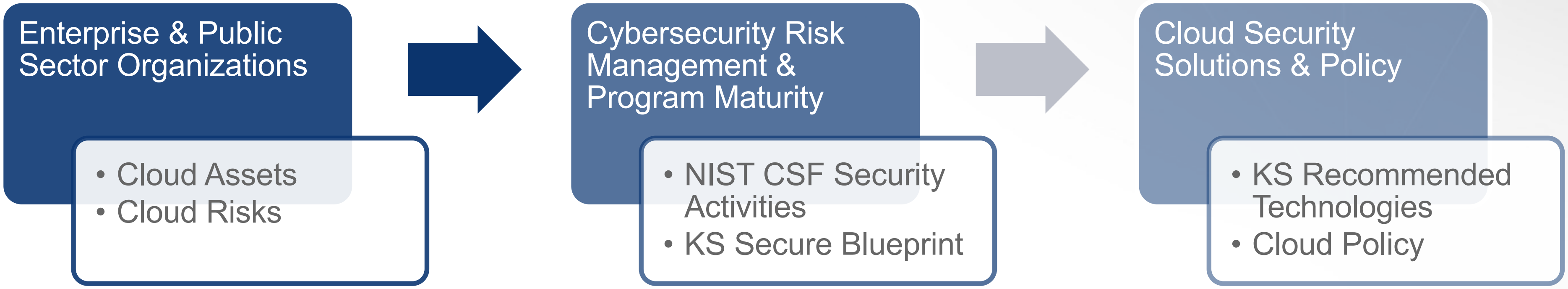
Cloud security is top of mind for CIOs and CISOs, faced with a changing technology paradigm in which control and security responsibility has become a shared concern. Widespread adoption of cloud services as a means of improving business efficiency naturally leads to an increase in the number and frequency of cloud-based cyber attacks.

The Kudelski Security Cloud Reference Architecture uses the widely recognized National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to identify security activities that are relevant to cloud, both software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS). These cloud security activities are categorized by their respective components from Secure Blueprint, Kudelski Security's unique strategic approach to cybersecurity program management.

To fulfil these cloud security activities and address cloud risks, we highlight cloud protection technologies from leading vendors that work in concert with the native security services from leading IaaS and SaaS providers. The highlighted technologies in this Cloud Reference Architecture are recommended based on our real-world experience evaluating, deploying, integrating, and managing these technologies. We believe that the vendors we highlight offer capabilities that can collectively provide a level of advanced cloud protection sufficient to help address the risks facing most organizations.

Together, the framework and technologies serve as a basis for more meaningful conversations with our clients that help them better understand their cloud risk posture as well as the capabilities and gaps of their incumbent security technologies in cloud environments.

Cloud Reference Architecture



Enterprise & Public Sector Organizations

- Cloud Assets
- Cloud Risks

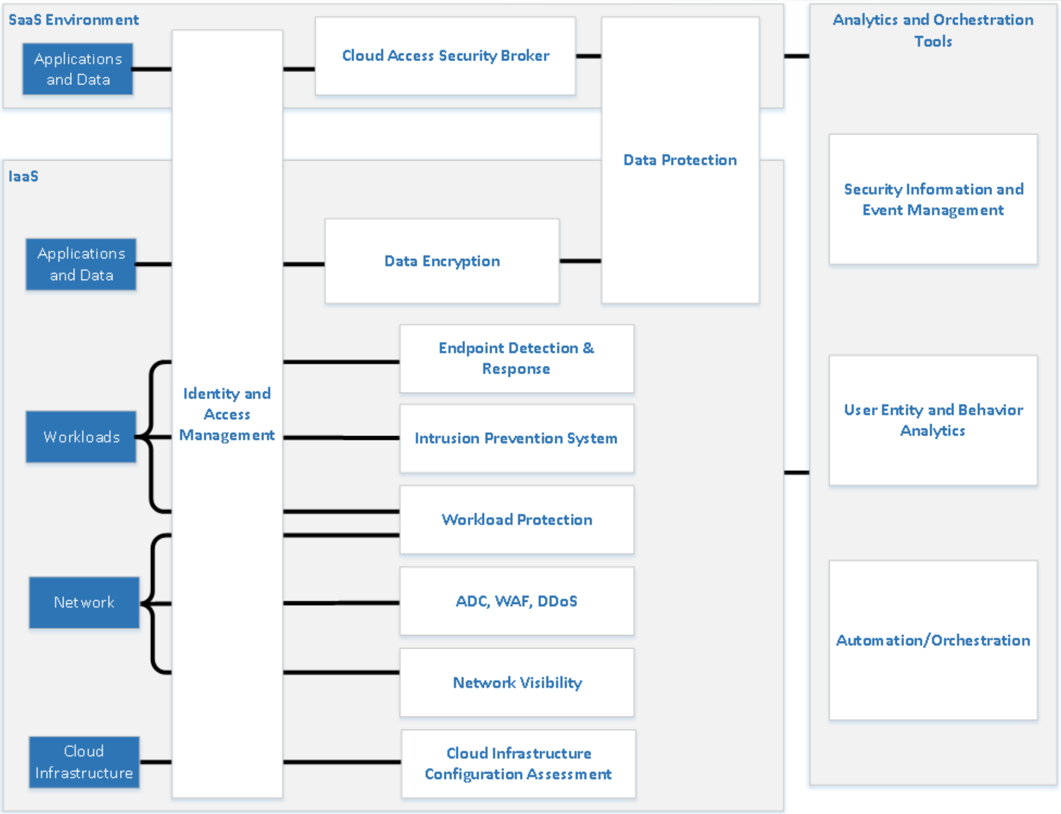
Cybersecurity Risk Management & Program Maturity

- NIST CSF Security Activities
- KS Secure Blueprint

Cloud Security Solutions & Policy

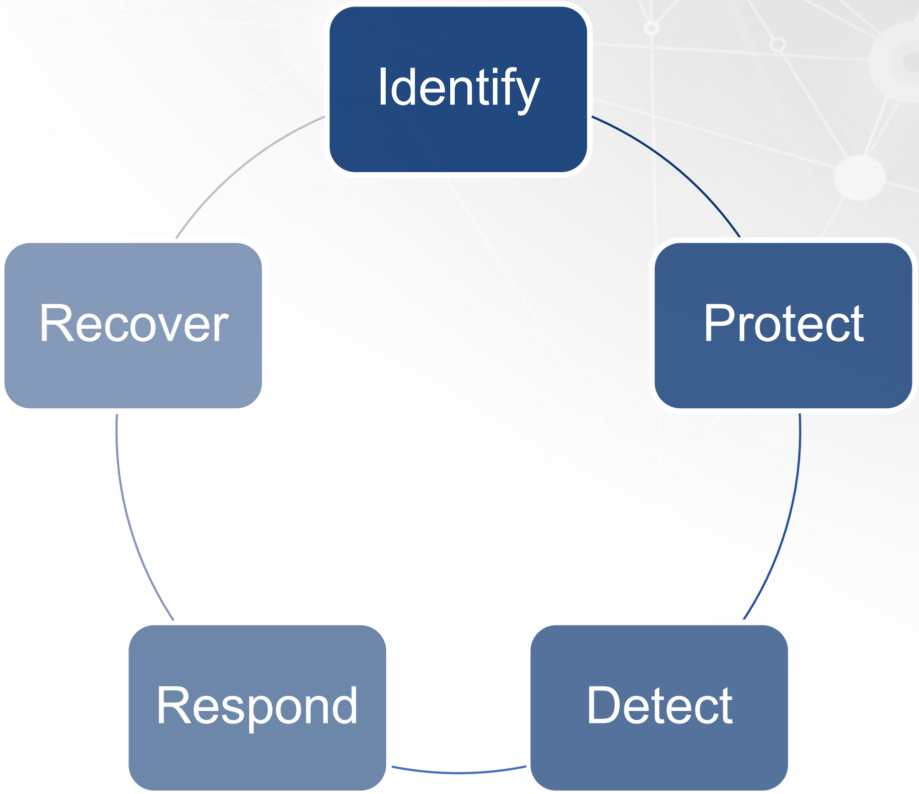
- KS Recommended Technologies
- Cloud Policy

Cloud Reference Architecture

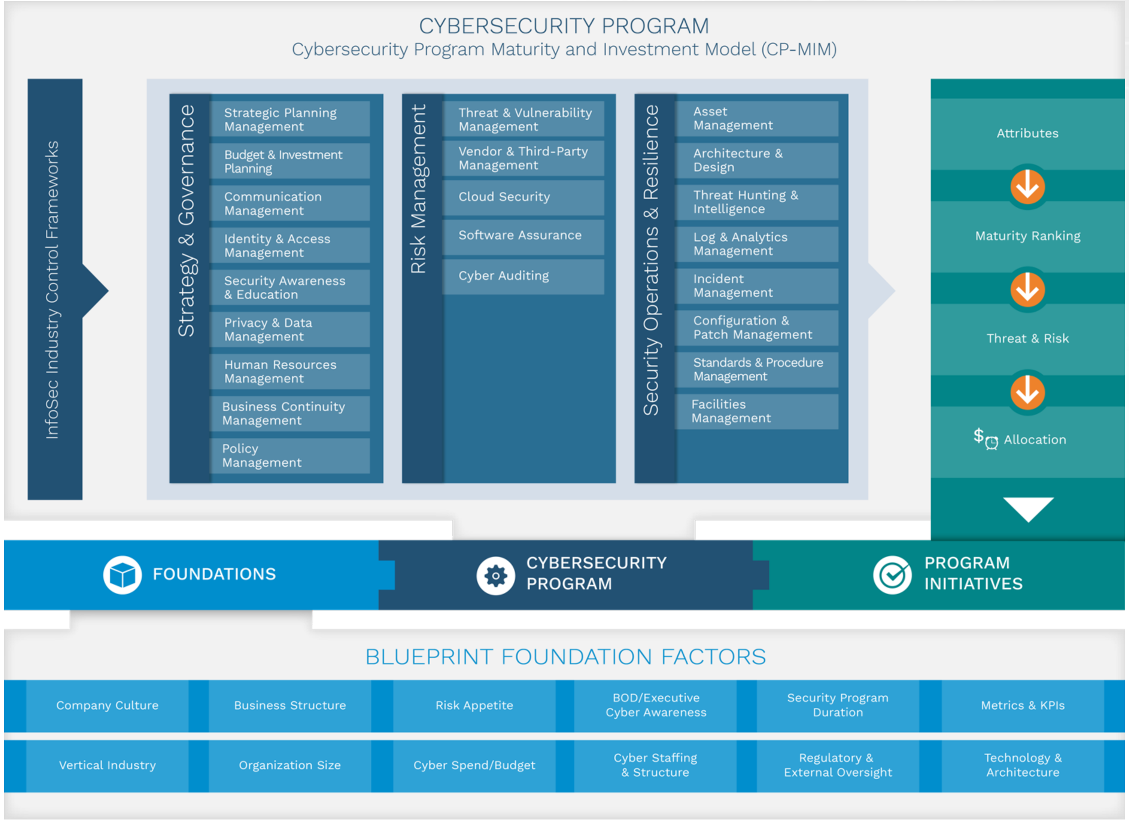

SaaS Environment
Applications and Data
Cloud Access Security Broker
Data Protection
Analytics and Orchestration Tools
IaaS
Applications and Data
Data Encryption
Security Information and Event Management
Workloads
Identity and Access Management
Endpoint Detection & Response
Intrusion Prevention System
Workload Protection
User Entity and Behavior Analytics
Network
ADC, WAF, DDoS
Network Visibility
Automation/Orchestration
Cloud Infrastructure
Cloud Infrastructure Configuration Assessment

NIST Cybersecurity Framework

- Voluntary, industry-led initiative to improve overall cybersecurity preparedness
- Risk-based, not control-based
- Flexible, risk-based methodology
- Supplements your existing cybersecurity frameworks



Secure Blueprint



CYBERSECURITY PROGRAM

Cybersecurity Program Maturity and Investment Model (CP-MIM)

InfoSec Industry Control Frameworks

Strategy & Governance
- Strategic Planning Management
- Budget & Investment Planning
- Communication Management
- Identity & Access Management
- Security Awareness & Education
- Privacy & Data Management
- Human Resources Management
- Business Continuity Management
- Policy Management

Risk Management
- Threat & Vulnerability Management
- Vendor & Third-Party Management
- Cloud Security
- Software Assurance
- Cyber Auditing

Security Operations & Resilience
- Asset Management
- Architecture & Design
- Threat Hunting & Intelligence
- Log & Analytics Management
- Incident Management
- Configuration & Patch Management
- Standards & Procedure Management
- Facilities Management

Attributes

Maturity Ranking

Threat & Risk

$ Allocation

FOUNDATIONS

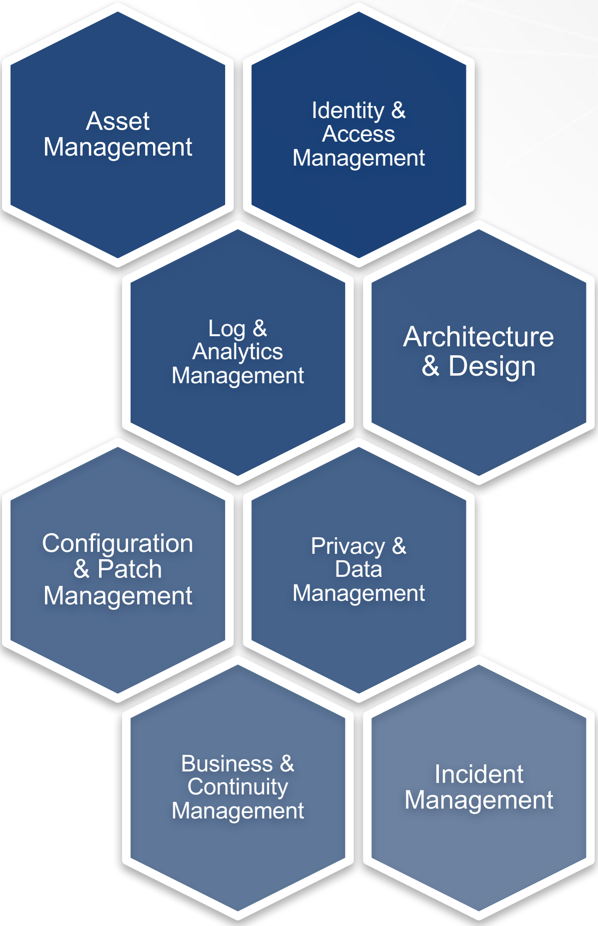
CYBERSECURITY PROGRAM

PROGRAM INITIATIVES

BLUEPRINT FOUNDATION FACTORS

Company Culture	Business Structure	Risk Appetite	BOD/Executive Cyber Awareness	Security Program Duration	Metrics & KPIs
Vertical Industry	Organization Size	Cyber Spend/Budget	Cyber Staffing & Structure	Regulatory & External Oversight	Technology & Architecture

Cloud Reference Architecture



Asset Management

Identity & Access Management

Log & Analytics Management

Architecture & Design

Configuration & Patch Management

Privacy & Data Management

Business & Continuity Management

Incident Management

Asset Management

- What cloud services? What data? What users?
- Understanding cloud utilization is a precursor to adequate technical and policy controls
- Organizations are under pressure to embrace cloud offerings and figure out how to integrate them as sanctioned business tools

Asset Management

Catalog External Information Systems

- What cloud assets are being used?

Map Organizational Communications and Data Flows

- How are cloud assets being used?

Prioritize Resources Based on Criticality and Business Value

- What is the relative business value and enterprise-readiness of a cloud asset?

KUDELSKI SECURITY

Identity & Access Management

- Over 80% of hacking-related breaches involve weak or stolen password (Verizon)

- Increased complexity and fractured user authentication resulting from:
  - Public Cloud Services
  - Social Media
  - API Token Management

Identity & Access Management

Manage Identities and Credentials for Authorized Users and Devices

- The convenience of single sign-on + the protection of adaptive multi-factor authentication
- Automated on-boarding/off-boarding and application usage analytics

Manage Access Permissions, Incorporating Least Privilege and Separation of Duties

- Fine-grained access control, including IaaS platforms

KUDELSKI SECURITY

Log and Analytics Management

- Visibility into cloud infrastructure security is one of the top three biggest headaches for IT security professionals (ISC^2)

- Cloud platforms generate a wealth of information about cloud activities

- Organizations may require a deeper level of visibility to meet regulatory or business objectives

KUDELSKI SECURITY

Log and Analytics Management

Aggregate and Correlate Event Data From Multiple Sources

- Ingest and correlate cloud and non-cloud events for a holistic view

Monitor the Network to Detect Potential Cybersecurity Events

- By 2020, 86% of all data center traffic will be within and between data centers (east-west traffic)

Monitor Personnel to Detect Potential Cybersecurity Events

- Can you monitor and detect risky user behavior across SaaS and IaaS platforms?

Detect Malicious Code

- Scalable endpoint protection for IaaS + visibility and detection for SaaS

Monitor for Unauthorized Connections, Devices, and Software

- Cloud-optimized host-based protections

Architecture and Design

- Abstracted networking concepts of the cloud require organizations to adapt their approach to cloud network architecture

- Hybrid and transitional cloud organizations may wish to maintain their investment and in-house expertise with traditional on premise technologies

Protect Network Integrity, Incorporating Network Segmentation Where Appropriate

- Instance-level micro segmentation, manageable at scale in a dynamic environment

KUDELSKI SECURITY

Configuration and Patch Management

- As with on premise assets, one of the most important steps you can take toward securing your cloud is patching and proper hardening

Create and Maintain a Baseline Configuration of Information Technology

- Configuration policies for SaaS, IaaS platforms, IaaS workload and deployed infrastructure
- Industry-standard templates (e.g. CIS, CSA)

Identify, Document and Mitigate Asset Vulnerabilities

- Lightweight and dynamic vulnerability management (e.g. CI/CD Pipeline)

Privacy and Data Management

- 74% of organizations reported storing some or all of their sensitive data in public clouds (McAfee)

- Data governance policy considerations for the cloud:
  - Lifecycle/Lineage
  - Metadata Management
  - Data Privacy Laws (e.g. GDPR)
  - Encryption/Tokenization

Privacy and Data Management

Protect Data-at-Rest

- Is your legacy encryption and key management sufficient?
- Is the cloud provider’s encryption and key management sufficient?

Protect Data-in-Transit

- Encrypting inter- and intra-cloud traffic, especially M2M

Protect Against Data Leaks

- 25 percent of “shadow data” is broadly shared internally, externally, and/or with the public (Symantec)

Business and Continuity Management

- Although IaaS platforms may be designed for multiple 9's of availability, it doesn't mean that your cloud-hosted applications are

- SaaS data loss is usually the result of accidental deletion, not catastrophic loss at the platform level

Conduct, Maintain, and Periodically Test Backups of Information

- Align IaaS and SaaS backup and retention policies to business and compliance requirements

KUDELSKI SECURITY

Incident Management

- Leverage native cloud capabilities
  - Quickly spin up a “clean room” using infrastructure-as-code
  - Perform forensics using instance snapshots

- Automate and orchestrate security tasks and incident response

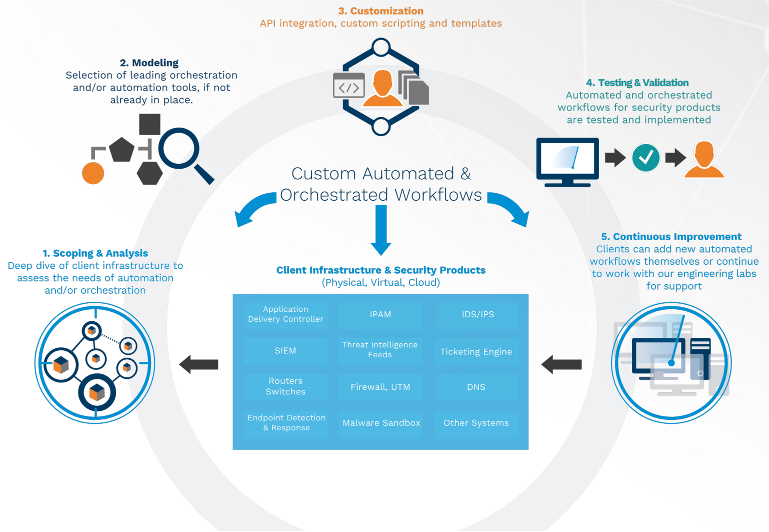
Contain & Mitigate Incidents

- Incident response teams must have the appropriate access, tools, processes, and training to contain and mitigate incidents in IaaS and SaaS

KUDELSKI SECURITY

Automation & Orchestration

- Increase agility and operational efficiency
- Reduce costs of repetitive tasks
- Increase accuracy and reduce downtime
- Amplify investments in existing technology through smart integration



3. Customization
API integration, custom scripting and templates

2. Modeling
Selection of leading orchestration and/or automation tools, if not already in place.

4. Testing & Validation
Automated and orchestrated workflows for security products are tested and implemented

Custom Automated & Orchestrated Workflows

1. Scoping & Analysis
Deep dive of client infrastructure to assess the needs of automation and/or orchestration

5. Continuous Improvement
Clients can add new automated workflows themselves or continue to work with our engineering labs for support

Client Infrastructure & Security Products
(Physical, Virtual, Cloud)

Application Delivery Controller	IPAM	IDS/IPS
SIEM	Threat Intelligence Feeds	Ticketing Engine
Routers Switches	Firewall, UTM	DNS
Endpoint Detection & Response	Malware Sandbox	Other Systems

Questions?

Thank You

Bo Lane
Head of Security Architecture
bo.lane@kudelskisecurity.com